ACCENT ELECTRONIC

Cod fiscal: 1003600023124
Cod TVA: 0500301

33/1 Bulgara str., Chisinau MD — 2001, Moldova, Tel: (+373) 022 577-984; e-mail: corporate@accent.md; www.accentelectronic.md

Specificație tehnica detaliata propusa la LOTUL I. „Licente antivirus”

Symantec Endpoint Protection (SEP) oferă o protecție superioară multistrat pentru a opri amenințările, indiferent de modul în care vă atacă punctele finale. SEP se integrează cu infrastructura de securitate existentă pentru a oferi răspunsuri orchestrate pentru a aborda rapid amenințările.

Solutia ofera protectia, a stațiilor de lucru fizice/virtualizate și servere fizice/virtualizate, pentru o periodă de 12 luni;
Licenta Endpoint Protection, Subscription License with Support, 1 YR include cantitatea de 750 statii

Symantec Endpoint Protection, oferă: protecție împotriva malware-ului, învățare automată avansată, analiză comportamentală, filtrare a reputației, prevenirea exploatării și a intruziunilor, înșelăciune, securitate poștală, securitate web, firewall, control dispozitiv, instrumente de eliminare antivirus, instrumente de recuperare, raportare, REST API-uri și integrare cu Capabilități inteligente de cloud amenințări Symantec.

Include, de asemenea, apărarea împotriva amenințărilor mobile, detectarea și răspunsul punctelor finale, protecții împotriva exploatărilor Active Directory, capacități de reducere a suprafețelor de atac, cum ar fi izolarea aplicației inteligente, izolarea comportamentală, aplicația control și protecții extinse ale sistemului de operare. Protejează toate punctele finale, inclusiv stații de lucru, laptopuri, telefoane mobile, tablete și servere și este compatibil cu Windows,

macOS, Linux, Android, iOS, VMware ESX, Citrix XenServer și alte mașini virtuale. Soluția este gestionată de la o consolă centralizată, care acceptă definiția granulelor politicile de management.

Soluția ofera protecție pentru stații de lucru și servere si suporta urmatoare edițiile de SO:

Operating system (desktop)

Windows 7 (32-bit, 64-bit; RTM and SP1)

- Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Embedded 8 Standard (32-bit and 64-bit)
- Windows 8.1 (32-bit, 64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (32-bit, 64-bit)
- Windows 8.1 update for August 2014 (32-bit, 64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit)
- Windows 10 (version 1507) (32-bit, 64-bit), including Windows 10 Enterprise 2015 LTSB
- Windows 10 November Update (version 1511) (32-bit, 64-bit)

Digitally signed by Cobîlaș Eugeniu
Date: 2021.07.22 14:49:06 EEST
Reason: MoldSign Signature
Location: Moldova

• Windows 10 Anniversary Update (version 1607) (32-bit, 64-bit), including Windows 10 Enterprise 2016 LTSB

• Windows 10 Creators Update (version 1703) (32-bit, 64-bit)

• Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit)

• Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit)

• Windows 10 October 2018 Update (version 1809) (32-bit, 64-bit), including Windows 10 Enterprise 2019 LTSC.

• Windows 10 May 2019 Update (version 1903) (32-bit, 64-bit)

• Windows 10 November 2019 Update (version 1909) (32-bit, 64-bit) (14.2 RU1 and later)

• Windows 10 20H1 (Windows 10 version 2004) (14.3 and later)

• Windows 10 20H2 (Windows 10 version 2009) (as of 14.3 RU1)

pentru Mac OS:

•Mac OS X 10.10, 10.11, macOS 10.12, 10.13

Linux Operating System (32-bit and 64-bit versions)

• Amazon Linux

• CentOS 6U3 - 6U9, 7 - 7U4; 32-bit and 64-bit; 32-bit and 64-bit

• Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit

• Fedora 16, 17; 32-bit and 64-bit

• Oracle Linux (OEL) 6U2, 6U4, 6U5, 7, 7.1, 7.2, 7.3

• Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U4

• SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 64-bit

• SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit

• Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit

Suport de protecție pe sistemele de operare server

Windows Server 2008 R2

• Windows Small Business Server 2011
• Windows Server 2012
• Windows Server 2012 R2
• Windows Server 2012 R2 update for April 2014
• Windows Server 2012 R2 update for August 2014
• Windows Server 2016
• Windows Server 2019
• Windows Server, version 1803 (Server Core) (14.2 and later)
• Windows Server, version 1809 (Server Core)
• Windows Server, version 1903 (Server Core) (14.2 RU1 and later)
• Windows Server, version 1909 (Server Core) (14.2 RU1 and later)
• Windows Server, version 2004
• Windows Server, version 20H2 (14.3 RU1)

Supported operating systems as of version 14.3 RU1:

• Amazon Linux 2
• CentOS 6, 7, 8
• Debian 9, 10 (14.3 RU2 and later)
• Oracle Enterprise Linux 6, 7, 8
• Red Hat Enterprise Linux 6, 7, 8
• SuSE Linux Enterprise Server 12.x, 15.x
• Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS

Supported kernels of Symantec Linux Agent (also lists supported minor Linux OS versions)

Supported operating systems for version 14.3 MP1 and earlier:

• Amazon Linux
• CentOS 6U3 - 6U9, 7 - 7U7, 8; 32-bit and 64-bit

• Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit

• Fedora 16, 17; 32-bit and 64-bit

• Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4

• Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2

• SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3,

64-bit

• SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit

• Ubuntu 12.04, 14.04, 16.04, 18.04 (as of 14.3); 32-bit and 64-b

Arhitectura de agent unic Symantec permite securitatea IT echipe pentru a adăuga tehnologie de securitate inovatoare cu simplificat implementare, ceea ce înseamnă că nu sunt necesari agenți noi. În plus, SEP acceptă multe medii, inclusiv acum IPv6.

Cerintele minim pentru sisteme linux permit instalare si operare complete a unui agent

• Intel Pentium 4 (2 GHz CPU or higher)
• 1 GB of RAM
• 7 GB of free space on the hard disk
Oferta support pentur medii virtuale si cloud de tip:

• Microsoft Azure

• Amazon WorkSpaces

• VMware WS 5.0, GSX 3.2 or later, ESX 2.5 or later

• VMware ESXi 4.1 – 5.5

• VMware ESX 6.0

• Microsoft Virtual Server 2005

• Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V

• Citrix XenServer 5.6 or later

• Virtual Box by Oracle

Linux Operating System

Ofera instrumente și tehnologii pentru loadbalancing pentru distriburiea sarcinii pe rețeaua de transmisie a datelor în procesul de schimb de date între clienți și serverul de custozi (sau servere)

33/1 Bulgara str., Chisinau MD — 2001, Moldova, Tel: (+373) 022 577-984; e-mail: corporate@accent.md; www.accentelectronic.md

About failover and load balancin . https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Managing-management-servers-sites-and-databases/setting-up-failover-and-load-balancing-v51660713-d15e4845/about-failover-and-load-balancing-v8360157-d15e4930.html

Instrumente încorporate pentru acțiuni de audit atât pe partea computerelor personale client, cât și pe serverul de control, cu posibilitatea de a exporta în continuare date de audit către sisteme și fișiere externe

Symantec Endpoint Protection (SEPM) acceptă baza de date Microsoft SQL Server. Baza de date conține informații despre politicile de securitate, setările de configurare, datele despre atacuri, jurnalele și rapoartele, Capacitatea de a face backup și de a restaura mediul de stocare adecvat, dacă este necesar, atât manual, cât și automat

Ofera instrument de gestionare a licențelor încorporate (licențe) cu posibilitatea activării centralizate a tuturor funcționalităților software pentru a proteja punctele finale cu licența (licențele) corespunzătoare. Opțiunea de a activa (sau dezactiva) manual licența (licențele) la fiecare punct final nu este permisă. ***(Licensing Symantec Endpoint Protection, insataltion guide pag. 134-139)***

Disponibilitatea unui instrumentului LiveUpdate policies pentru livrarea actualizărilor la semnăturile bazelor de date antivirus, setări (politici) etc.

Symantec ofera seturi de instrucțiuni si ghidare pentru porcesul de instalare și administrare în limbile engleza, rusă, Italian, chineza, germana, etc.

Disponibilitatea unor instrumente gratuite suplimentare (sau funcționalitate încorporată) cu astfel de funcționalități:

- instrumentariu care permite trimiterea în mod automat a pachetelor de date cu mostre de fișiere infectate de la calculatoarele client în carantină centrală fără acces direct la calculatorul client în sine. **CentralQ (12.1.6 and earlier)**
- instrumentariu care permite o curățare completă a sistemului computerului client de software pentru a proteja acestea în caz de șită de către instrumentele standard ale sistemului de operare; https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Monitoring-Reporting-and-Enforcing-Compliance/setting-up-host-integrity-v33444962-d57e99.html
- instrumentariu care permite gestionarea și monitorizarea furnizorilor de actualizări în infrastructură bazat pe software de protecție a punctelor finale; **ContentDistributionMonitor (SEPMMonitor) + LiveUpdate Administrator**
- instrumentariu care vă permite să obțineți informații extinse despre dispozitive externe și anume: informații despre producător, model, număr de serie; https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/about-application-control-system-lockdown-and-devi-v36534292-d45e176/managing-device-control-v36640615-d45e108/obtaining-a-device-vendor-or-model-for-windows-com-v13650794-d75e1230/about-device-ids-v15861481-d75e1187.html
- instrumentariu care vă permite să integrați, prin API-uri deschise, un server centralizat pentru gestionarea parametrilor și setărilor de protecție împotriva amenințărilor pe stațiile de lucru client cu aplicații (sisteme) de monitorizare și gestionare la distanță (RMM) (sisteme de monitorizare și gestionare la distanță (RMM)) https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/Whats-new-for-Symantec-Endpoint-Protection-14_3-RU2.html

- instrumentariu pentru furnizarea de date analitice avansate bazate pe baza de date a serverului pentru gestionarea setărilor de protecție împotriva amenințărilor și a setărilor de pe stațiile de lucru client, inclusiv în formă grafică;
- instrumentariu pentru citirea simplificată a meniurilor și casetelor de dialog de pe server pentru gestionarea setărilor de protecție împotriva amenințărilor și a setărilor de pe stațiile de lucru ale clienților pentru persoanele cu dizabilități; -
- instrumentariu pentru extragerea și restaurarea fișierelor din mediul local de carantină dacă fișierul a fost pus în carantină din greșeală;- https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/virus-and-spyware-protection-dialog/quarantine-general-v43862145-d49e10943.html
- instrumentariu pentru actualizarea automată a parametrilor de comunicație între computerele client și serverul de control în cazul încetării unei astfel de comunicări din cauza mutării clientului către un alt domeniu, mutarea serverului de control și altele asemenea; - https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-the-client-server-connection-v26173180-d15e3300/how-does-the-client-computer-and-the-management-se-v15455169-d19e661.html
- instrumentariu pentru diagnosticarea avansată a problemelor, care colectează date și detectează problemele obișnuite pentru continuarea ascensiunii către asistența producătorului instrumentariu pentru diagnosticarea bazei de date a serverului de management. **Symantec Endpoint Protection Manager**
- https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/troubleshooting-v58233805-d77e6/troubleshooting-computer-issues-with-the-symantec-v20943682-d77e380.html

Capacitatea de a gestiona centralizat protecția antivirus pe toate computerele client, indiferent de sistemul de operare utilizat pe acestea (în conformitate cu lista de sisteme de operare acceptate).

Suportă gestionarea centralizată utilizând un server de management dedicat, cu posibilitatea de a vă conecta la panoul de control al serverului utilizând un browser web.

Suportă gestionarea centralizată utilizând un server de management dedicat, cu posibilitatea de a se conecta la serverul de adiministrare utilizând consola de Manager Client

Serverul de management trebuie sa fi instalat pe sistemul de operare Windows Server.

single agent architecture
Push Deployment Wizard - Posibilitatea de a instala de la distanță agenții pe stațiile de lucru cu sistemele de operare Windows într-un mod nesupravegheat (fără nicio acțiune a utilizatorilor).

- Microsoft Systems Management Server;
- IBM Tivoli;
- Novell ZENworks.

Password-protecting the Symantec Endpoint Protection client

Posibilitatea de auto-creare a pachetelor de instalare (instalatori) cu parametrii necesari (inclusiv module de protecție) pentru stațiile de lucru.

Baza de date SQL Server este instalată automat cu Symantec Endpoint Protection Manager în mod implicit.

Ofera Capacitatea de a construi o structură ierarhică de administrare de pe mai multe servere, atât pe un singur site, cât și situate în rețele diferite și geografic la distanță.

Atunci când serverele sunt distribuite in rețele diferite și la distanță geografică, este necesar să existe o tehnologie încorporată de replicare a datelor între astfel de servere, în timp ce replicarea trebuie să fie acceptată atât în modurile manuale, cât și în cele automate
Gestionați setările de carantină ca parte importantă a strategiei dvs. de focar de virus.

Atunci când virusul și spyware-ul scanează sau SONAR detectează o amenințare, Symantec Endpoint Protection plasează fișierele suspecte în carantina locală a computerului infectat. Clientul fie repară fișierul, îl repară și îl restabilește, fie îl șterge.

Când clientul detectează un risc și pune în carantină fișierul, acesta notifică serverul de administrare. Puteți activa serverul de administrare să solicite și să recupereze automat fișierul în carantină. Serverul de gestionare încarcă și stochează probe de risc în baza de date, afișează detaliile evenimentului și vă permite să le descărcați pentru analize suplimentare. Poate doriți să trimiteți fișierul către echipa dvs. internă de malware sau de securitate pentru inginerie inversă sau către un alt sandbox pentru analiză. Dacă credeți că condamnarea este fals pozitivă, contactați Asistența Symantec pentru a înregistra un caz.

Posibilitatea de scanare anti-virus pe stațiile de lucru cu cerința de utilizator sau administrator, în modul manual

Prezența tehnologiei incorporate în antivirus care vă permite să excludeți de la scanarea fișierelor incluse în imaginea standard a unei mașini virtuale, care sunt utilizate pentru a clona (a crea noi) mașini virtuale;

Tehnologie de accelerare a scanării care vă permite să depășiți scanările programate și manuale ale fișierelor care au fost deja scanate de alte computere client din aceeași rețea.

Actualizarea manuală sau la timp a bazelor de date antivirus, a regulilor (politicilor). Abilitatea de a aplica reguli de actualizare diferite pentru diferite grupuri de clienți.

Capacitatea de a defini parametrii detaliați ai scanerului antivirus, precum: definirea obiectelor și metodele de scanare, capacitatea de a seta dimensiunea și timpul maxim pentru scanarea unui fișier, adâncimea maximă de pastrare a arhivelor și crearea de excepții;

Abilitatea de a reveni la versiunile anterioare ale bazelor de date de semnături.

Posibilitatea de a primi actualizări de baze de date de viruși din surse de rezervă dacă sursa principală de actualizare nu este disponibilă.

Capacitatea de a actualiza bazele de date antivirus atât de pe serverul de control, cât și direct de la serviciul producătorului de software pentru protejarea stațiile de lucru.

Abilitatea de a utiliza ca surse intermediare de actualizări și distribuirea politicilor și setărilor oricărui computer client ca furnizor de actualizări pentru un grup de clienți specificați.

Capacitatea de a primi actualizări pentru semnăturile de viruși și politicile clientului prin mijloace alternative (instrumente terțe) prin rețeaua locală de date (IBM Tivoli, Microsoft SMS etc.).

Disponibilitatea instrumentelor pentru identificarea computerelor client neprotejate (care nu au software pentru a proteja locurile de muncă finale).

Ofera un system modular de protecție pe mai multe niveluri cu următorii parametri:

- protecție la nivel de rețea (firewall)
- protecție împotriva intruziunii (IPS)
- protecție la nivel de sistem de fișiere;
- protecție bazată pe reputația fișierelor;
- protecție bazată pe comportamentul proceselor generate de programe;

un instrument pentru repararea și restaurarea sistemului de operare, dacă acesta este deja infectat.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html

Capacitatea integrare cu sistemele de securitate a perimetrului rețelei folosind API-uri.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/release-notes/Whats-new-for-Symantec-Endpoint-Protection-14_3-RU2.html

Capacitatea de sisteme de securitate perimetrale de rețea bazate pe cloud de la același producător.

Posibilitatea de integrare cu produsul * de la același producător, care permite efectuarea unei protecții extinse complexe, monitorizare și analiză împotriva amenințărilor de toate tipurile la toate nivelurile de infrastructură (lucrări finale, rețele locale și web și servere de poștă).

* Notă: acest produs trebuie să aibă:

- sandbox încorporat și cloud pentru analiza amenințărilor;
- căutarea și identificarea amenințărilor de zi „zero”, a atacurilor de hash;
- capacitatea de a exporta date către soluții SIEM terțe;
- un instrument de vizualizare pentru indicatorii de protecție (Indicatori de compromis - IoC), incluzând o reprezentare grafică completă a interacțiunii dintre aceștia (de exemplu, un lanț din forma „fișiere implicate în atac” - „adrese IP din care au fost descărcate fișierele” - „utilizatori afectați de atacuri "-" calea distribuției către alți utilizatori "etc.);

să fie capabil să blocheze linkurile malicioase din e-mailuri în etapa de livrare a scrisorii către utilizator.

Existența unui mecanism de detectare a conformității sau a neconformității cu criteriile specificate pentru prezența corecțiilor de securitate (patch-uri) în sistemul de securitate al sistemului de operare la stațiile de lucru.

Disponibilitatea tehnologiei permite reducerea volumului de semnături antivirus stocate pe stațiile de lucru client de cel puțin două ori, prin studierea reputației fișierelor prin mediul cloud existent al producătorului. Atunci când examinați reputația unui fișier, numai detaliile fișierului, cum ar fi dimensiunea acestuia, data creării, hash etc., ar trebui transferate în cloud, nu fișierul în sine.

Functionalitati de protecție:

Disponibilitate de protecție împotriva: rootkit-uri, programe malware, spyware, troieni, adware, criptare, software potențial nedorit și periculos, atacuri de rețea și spam.

Suport pentru această protecție atât pentru PC-uri fizice, cât și pentru medii virtuale (VDI, sesiuni de terminal etc.).

Posibilitatea de a crea excepții pentru a căuta amenințări (viruși) ale următoarelor elemente ale sistemului de operare Windows: fisier;

- catalog;
- amenințări cunoscute;
- extensie de fișier;
- domeniu;

anexă.

Disponibilitatea protecției împotriva atacurilor și amenințărilor care se răspândesc prin rețelele web și locale, serviciile de e-mail, mass-media amovibilă, inclusiv:

- protecție împotriva amenințărilor precum „botnet”;
- protecție împotriva falsificării IP și MAC;
- protecție împotriva amenințărilor de zi „zero”;
- protecție împotriva amenințărilor care pot exploata vulnerabilitățile în Java, Flash și alte aplicații;

protecție împotriva amenințărilor mascate în pachete (de exemplu, arhive de instalare).

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/what-is-v45096464-d43e1648/how-symantec-endpoint-protection-technologies-prot-v97539434-d43e1669.html

Suport pentru tehnologia anti-exploit în memoria computerului bazată pe tehnologii de vulnerabilitate cunoscute:

- prevenirea executării codului JAVA în afara sandbox-ului, inclusiv - dezactivarea Managerului de securitate JAVA
- Prevenirea suprascrierii cadrelor Structured Exception Handler (SHE) în memoria computerului pentru a intercepta handlerul SEH în Windows;

Prevenirea executării programelor (aplicațiilor) care pot provoca depășirea spațiului de adrese („heap”) în memoria computerului.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/hardening-windows-clients-against-memory-tampering-v123149922-d3859e12879/memory-exploit-mitigation-techniques-v114221375-d53e13441.html

Asigurarea protecției în timp real.

Pentru stațiile de lucru cu sistemele de operare Windows, este disponibili mecanism de scanare a fișierelor în timp real cu analiza simultana pe baza analizei euristice, a învățării automate și a datelor de reputație.
Acest motor de scanare ar trebui să poată adăuga codul său la aplicațiile care rulează exclusiv în modul utilizator Windows (UMH) pentru a analiza comportamentul acestei aplicații și a o închide imediat în caz de activitate rău intenționată.
https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/managing-scans-on-client-computers-v40739504-d49e6/about-the-types-of-scans-and-real-time-protection-v41160104-d49e2232.html
Suport pentru scanarea antivirus a mediilor amovibile în modul automat și manual.

Este obligatoriu să dispuna de un driver special pentru pornirea timpurie a sistemului ELAM, care protejează computerele client în timpul startarii

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/managing-early-launch-anti-malware-elam-detections-v71631870-d49e1545.html

Posibilitatea de a scana fișiere la pornirea sistemului (inclusiv sectorul de boot, RAM), în timpul operațiilor de fișiere, în modul manual și în timp.

Tehnologie încorporată care monitorizează aplicațiile și fișierele care încearcă să modifice setările DNS (inclusiv fișierul gazdă de pe computerul client).

Abilitatea de a verifica conținutul arhivelor cu posibilitatea de a regla profunzimea unei astfel de verificări.

Existența modulului de protecție împotriva spamului și a altor amenințări cu posibilitatea integrării în clientul de poștă electronică.

Posibilitatea de a instala agentul pe o stație de lucru cu sau fără modul curent (pentru punctele finale care nu utilizează clienți de e-mail).

Verificarea traficului HTTP, FTP, POP, SMTP, IMAP, inclusiv a canalelor de transmisie de date criptate. https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-fw-console-v9393553-d53e5522/protection-and-stealth-settings-v8240375-d53e7191.html

Prezența unui firewall personal, care conține un master pentru crearea reguli și editor pentru zonele de rețea cu posibilitatea de a crea diferite profiluri pentru un firewall personal, care poate fi comutat automat în funcție de condițiile de utilizare ale stațiilor de lucru (la care rețea este conectat stația de lucru, prin care interfață este conectat stația de lucru și etc.).

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-firewall-protection-v15703943-d53e474/about-the-firewall-v42226922-d53e881.html

Abilitatea de a restricționa accesul la anumite categorii de site-uri pe baza regulilor firewall în conformitate cu următoarele criterii:

- o aplicație care utilizează accesul la Internet;
- protocol utilizat;

- adaptorul de rețea utilizat.

În același timp, restricționarea accesului la anumite categorii de site-uri ar trebui setată atât de adresa IP, cât și de numele DNS al domeniului sau gazdei.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-firewall-protection-v15703943-d53e474.html#v15703943

Sistem de detectare și prevenire a intruziunilor (IDS sau IPS) care protejează computerul de malware și de activități nedorite.

Capacitatea de a detecta și preveni intruziunile (cu blocarea descărcării și executării obiectelor rău intenționate) la diferite niveluri ale modelului de rețea OSI (de la rețeaua [2] la aplicația [al șaptelea] strat) pentru Windows.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-intrusion-prevention-v36820771-d53e8657/about-symantec-ips-signatures-v36817114-d53e9297.html

Capacitate obligatorie de a vă crea propriile semnături pentru sistemul de prevenire a intruziunilor.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/managing-intrusion-prevention-v36820771-d53e8657/managing-custom-intrusion-prevention-signatures-v37711224-d53e8845/creating-a-custom-ips-library-v38553637-d53e9900.html

Capacitatea de a exclude anumite stații de lucru de la scanarea de către sistemul de detectare și prevenire a intruziunilor și o astfel de excludere trebuie setată în conformitate cu următoarele criterii: adresă IP, interval de adrese IP sau mască de subrețea.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/exceptions-v8093021-d51e2316/exceptions-v8553565-d51e2388.html

Prezența unor tehnologii care permit analizarea fișierelor în vederea reputației și emiterea unui verdict asupra prejudiciului sau siguranței acestora. Tehnologia bazată pe reputație ar trebui să se bazeze pe informații localizate și analizate constant în mediul cloud al producătorului.

Notă: reputația reprezintă informații despre câte computere din lume este prezent acest fișier, cât timp a existat, prin ce canale de comunicare și din ce resursă a fost primit și cu ce resurse interacționează etc.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/preventing-and-handling-virus-and-spyware-attacks-v40739565-d49e172/how-uses-symantec-insight-to-make-decisions-about-v45204303-d49e3040.html

Disponibilitatea propiei tehnologiei (instrumentariu) implementat efectiv pentru controlul și gestionarea autorizațiilor pentru:

- lansarea aplicațiilor predefinite;
- accesul sau încetarea proceselor specificate;
- acces la fișiere, chei de registry și biblioteci din aplicații specificate.

Această tehnologie ar trebui să poată crea propriile reguli în conformitate cu următoarele criterii:

- suport pentru sistemul de operare Windows și browserele EI, Egde, Firefox;
- posibilitatea de a folosi măști de substituție (simboluri „*”, „?” etc.);
- capacitatea de a specifica unde ar trebui să funcționeze aceste reguli (unități locale, unități de rețea, suporturi amovibile etc.);
- capacitatea de a stabili condiții pentru diferite tipuri de operațiuni de intrare-ieșire (citire, scriere, modificare etc.);
- capacitatea de a crea excepții.

Tehnologia proprietară (instrument) pentru controlul și gestionarea permisiunilor pentru a rula aplicații și pentru a accesa fișiere și procese trebuie să fie integrată în software-ul de protecție a punctelor finale (să fie o parte integrantă a produsului).

https://knowledge.broadcom.com/external/article/155455/block-or-allow-devices-using-endpoint-pr.html

Posibilitatea de a bloca software-ul cu:
- „liste albe” bazate pe amprente „digitale” folosind tehnologia de calcul sumă hash (adică liste de aplicații care pot rula, în timp ce orice alte programe nu vor fi disponibile pentru a rula)

“liste negre” bazate pe amprente digitale folosind tehnologia de calcul sumă hash (adică liste de aplicații care nu vor putea rula, în timp ce orice alte programe vor fi disponibile pentru a rula).
https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/testing-policies-v99640437-d55e2211/adding-and-testing-a-rule-that-blocks-a-dll-v99640361-d55e2994.html
Disponibilitatea propriei tehnologiei incorporate efficiente pentru controlul suporturilor amovibile cu capacitatea de a crea reguli pentru:

- tipul dispozitivului;
- producătorul dispozitivului;
- modelul și numărul de serie al dispozitivului.

Disponibilitatea propriei tehnologiei incorporate efficiente pentru controlul suporturilor amovibile ar trebui să fie integrată în software-ul de protecție a punctelor finale (să fie o parte integrantă a produsului).

Posibilitatea de a căuta în Windows după ID-ul clasei sau ID-ul dispozitivului în funcție de șabloane (folosind asteriscul „*”).

Capacitatea de a căuta în MacOS prin expresii regulate care pot utiliza caractere:

- . (Punct)
- \ (backslash)
- [set], [^ Set] (set)
- * (asteriscuri)

+ (plus).

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-appdevicecon-console-v9395464-d45e3203/device-control-v8240526-d45e4485.html

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-appdevicecon-console-v9395464-d45e3203/system-lockdown-for-v9209197-d45e3206.html

Disponibilitatea propriei tehnologiei incorporate efficiente pentru instalarea forțată centralizată a actualizărilor de securitate (inclusiv patch-uri Windows Update) pe stații de lucru cu sistem de operare Windows.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Monitoring-Reporting-and-Enforcing-Compliance/setting-up-host-integrity-v33444962-d57e99/about-host-integrity-requirements-v10869719-d57e191.html

Disponibilitatea propriei tehnologiei incorporate efficiente pentru blocarea fișierelor după numele sau extensia specificată.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-appdevicecon-console-v9395464-d45e3203/file-and-folder-access-attempts-properties-v8240505-d45e3975.html

Cerințe de administrare și audit:

Disponibilitatea managerului de utilizatori, care vă permite să creați utilizatori diferiți ai serverului de administrare (administratori, operatori etc.) și să le atribuiți diferiți drepturi de acces la partiții individuale, grupuri de computere de pe serverul de administrare.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-groups-clients-and-administrators/managing-groups-of-clients-v26125981-d19e6/how-you-can-structure-groups-v8970377-d19e2300.html

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-admin-page-administrators-v14650809-d1e2474/group-rights-v8573512-d1e3116.html

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/performing-the-tasks-that-are-common-to-all-polici-v15703889-d55e6/assigning-a-policy-to-a-group-or-location-v15703893-d55e1116.html

Abilitatea de a controla de la distanță serverul de administrare folosind un browser web cu posibilitatea de a furniza astfel acces la adrese IP specifice ale utilizatorilor.

Prezența unei reviste în care:

- toate modificările în configurație și toate acțiunile efectuate de utilizatorii serverului de administrare sunt monitorizate și înregistrate;
- Urmărirea evenimentelor legate de acțiuni pe stații de lucru.
- Urmărirea evenimentelor legate de activitatea rootkiturilor, malware, spyware, troieni, adware, software criptat, potențial nedorit și periculos, atacuri de rețea și spam, etc.

Posibilitatea de a crea evenimente personalizate cu jurnalizare și mesaje suplimentare prin e-mail către persoane responsabile.

Posibilitatea de a salva jurnalele pe stațiile de lucru pentru analize suplimentare sau tipărirea unui astfel de jurnal.

Prezența funcționalității încorporate în serverul de gestionare care vă permite să setați volumul (dimensiunea) și parametrii de stocare a jurnalelor la stațiile de lucru finale pentru evenimente de sistem, evenimente legate de amenințări, trafic de rețea

Prezența unui panou web, care face posibilă monitorizarea stării protecției antivirus a rețelei corporative în timp real și oferă informații actualizate despre starea de securitate.

Este imperative ca solutia sa dispuna de propriul serviciu web care vă permite să vizualizați jurnalele folosind browserele web în lunile de lucru la distanță.

Suport obligatoriu pentru un protocol criptat pentru astfel de acțiuni cu un port separat, care poate fi setat de administratorul de sistem în setările serverului de administrare.

Integrare cu Active Directory și / sau LDAP.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-admin-page-servers-databases-v14650805-d3e3/add-directory-server-general-v53779509-d3e688.html

Suportă autentificarea factoriala dubla RSA SecurID pentru a proteja conturile de administrator

https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-groups-clients-and-administrators/managing-administrator-accounts-v17364367-d1e6/choosing-the-authentication-method-for-administrat-v9542292-d1e613/using-rsa-securid-authentication-with-v11030623-d1e748.html

Prezența unui mecanism încorporat (instrumente) pentru crearea și restaurarea copiilor de rezervă ale serverului de administrare (inclusiv baza de date pe care rulează serverul).

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Managing-management-servers-sites-and-databases/disaster-recovery-best-practices-for-endpoint-prot-v18588940-d15e2803/restoring-the-database-v18655541-d15e584.html

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/upgrading-to-a-new-release-v14510472-d27e6/Restoring-replication.html

Posibilitatea de a crea un fișier dedicat de recuperare de urgență (cu parole de criptare, ID de domeniu al fișierelor de depozitare de chei, fișiere de certificate, licențe etc.).

Abilitatea de a crea diferite grupuri de utilizatori cu parametri (diferiți) separați (reguli, module de securitate etc.). Abilitatea de a aplica politici ca pentru toți utilizatorii simultan și pentru grupuri individuale.

Disponibilitatea instrumentelor pentru editarea grupurilor de utilizatori, care permite:

- crearea, editarea,ștergerea grupuri de utilizatori;
- importarea grupuri din Active Directory și crearea un arbore similar de grupuri;

efectuarea sincronizării periodică a grupurilor configurate cu Active Directory.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-groups-clients-and-administrators/managing-groups-of-clients-v26125981-d19e6.html

Capacitatea de a crea politici separate pentru fiecare tip de protecție (protecție antivirus, firewall, IPS etc.).

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/performing-the-tasks-that-are-common-to-all-polici-v15703889-d55e6/editing-a-policy-v39225639-d55e827.html

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-policies-console-v14650832-d55e3377/policies-v45279486-d55e3564.html

Abilitatea de a exporta / importa politici într-un fișier separate

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Using-policies-to-manage-security/performing-the-tasks-that-are-common-to-all-polici-v15703889-d55e6/exporting-and-importing-individual-endpoint-protec-v39329564-d55e1456.html

Capacitatea de a construi un set de pachete de instalare pentru instalarea lor ulterioară pe stații de lucru, inclusiv pachete pentru diverse sisteme de operare, diverse versiuni de software pentru protejarea locurilor de muncă finale.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-admin-page-install-packages-v14650803-d21e4696/client-install-packages-overview-v8429228-d21e4699.html

Posibilitatea instalării centralizate a agenților pe stații de lucru (inclusiv un grup de stații) utilizând tehnologia „push”.
Posibilitatea de a trimite un link către locația pachetelor de instalare prin e-mail în scopul instalării manuale a pachetului pe locurilor de muncă finale.
https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/getting-up-and-running-on-for-the-first-time-v45150512-d43e1033/installing-clients-with-remote-push-v16194683-d21e1695.html
Posibilitatea aplicării centralizate a politicilor pe stații de lucru atât pentru stații în ansamblu, cât și pentru utilizatorii săi individuali.

Abilitatea de a activa și dezactiva de la distanță module de protecție precum firewall personal, protecție în timp real, protecție client e-mail, protecție acces internet, control web și multe altele
Capacitatea de a rula de la distanță pe stații de lucru proceduri legate de protecția punctelor finale, cum ar fi scanarea, actualizarea politicilor și altele asemenea.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-console-lu-settings-policy-v25075140-d79e5424/group-update-provider-v8429565-d79e5782.html

Disponibilitatea instrumentelor pentru configurarea programului pentru actualizările de semnături și politici ale software-ului antivirus pe stații de lucru.

Având un instrument pentru a identifica mașinile virtuale invitate care au un agent software de protecție a punctelor finale instalat ca clienți temporari. Prezența unor astfel de oportunități este obligatorie:

- stabilirea perioadei de îmbătrânire pentru astfel de mașini virtuale;

eliminarea automată a agenților pe astfel de mașini virtuale (marcată ca temporară) odată cu eliberarea simultană a licenței după o perioadă de îmbătrânire specificată.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-help-console-lu-settings-policy-v25075140-d79e5424/group-update-provider-v8429565-d79e5782.html

- ***Întregul volum al licentelor este furnizat impreuna cu support tehnic de la producător pentru o perioadă de cel puțin 12 luni din momentul furnizarii licentelor prin posta electronica si activarii precum si semanrii actului de predare a licentelor.**
- ***Dreptul de a utiliza software-ul propus este exclussiv pentru un an. Cu cel putin trei luni inainte de expirare furnizorul va informa clientul despre necessitate de reinoire a licentelor si prelungire a supotrului.**
- ***Producătorul ofera suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului pe perioade dispunerii licentelor active**
- ***Certificatelor de conformitate ISO 27001 și ISO 9001 ale ofertantului, valabile se anexeaza la oferta.**
- ***Autorizatia de la producator a ofertantului este anexata.**